TUNNEL FET BASED ENERGY EFFICIENT CIRCUIT DESIGN WITH ENHANCED HARDWARE SECURITY

Synopsis of the Thesis to be submitted in Partial Fulfillment

of the Requirements for the Award of the Degree of

Doctor of Philosophy

by

JAPA ADITYA
(Roll No: 165010101)

Under the Supervision of

Dr. Manoj Kumar Majumder
&
Dr. Subhendu K. Sahoo

Department of Electronics and Communication Engineering

International Institute of Information Technology Naya Raipur

Raipur – 493661

April, 2021

International Institute of Information Technology Naya Raipur

Declaration by the Student

Date: 29/04/2021

Title of the Thesis: Tunnel FET based Energy Efficient Circuit Design with Enhanced Hardware Security

I Certify that

a. the work contained in the thesis is original and has been done by me under the guidance of my Supervisor;

b. the work has not been submitted to any other Institute for any degree or diploma;

c. I have followed the guidelines provided by the Institute in preparing the thesis;

d. I have conformed to ethical norms and guidelines while writing the thesis and;

e. whenever I have used materials (data, models, figures, and text) from other sources, I have given due credit to them by citing them in the text of the thesis, giving their details in the references, and taking permission from the copyright owners of the sources, whenever necessary.

Signature of the Student: J. Aditya

Name of the Student: Japa Aditya (165010101)

डॉ. श्यामाप्रसाद मुखर्जी अंतरराष्ट्रीय सूचना प्रौद्योगिकी संस्थान
DR. SHYAMA PRASAD MUKHERJEE INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY, NAYA RAIPUR
(A Joint Initiative of NTPC & Govt. of Chhattisgarh)

Email: iiitnr@iiitnr.ac.in
Tel: +91-771-2474040
Web: www.iiitnr.ac.in

Declaration by the Supervisor(s)

This is to certify that the thesis entitled **Tunnel FET based Energy Efficient Circuit Design with Enhanced Hardware Security**, submitted by **JAPA ADITYA** to International Institute of Information Technology, Naya Raipur, is a record of bonafide research work under my (our) supervision and I/we consider it worthy of consideration for the Synopsis of the Thesis to be submitted in partial fulfillment of the requirements for the award of the degree of Doctor of Philosophy of the Institute.

MKM

Supervisor
Dr. Manoj Kumar Majumder

Subhendu Kumar Sahoo

Co-Supervisor
Dr. Subhendu K. Sahoo

Date: 29/04/2021

Abstract

This work proposes emerging tunnel FET (TFET) based energy efficient circuits for hardware security applications. Initially, TFET digital buffer, ring oscillator (RO), and voltage controlled ring oscillator (VCRO) designs have been proposed. TFET based buffers achieve 16× lower energy consumption with higher reliability compared to FinFET buffers. In addition, TFET based RO and VCRO exhibit higher frequency and large tuning range (90%) compared to FinFET designs. Moreover, to avoid the impact of p-i-n forward current, different circuit techniques have been demonstrated that achieve at least 2× lower power consumption and higher reliability compared to the conventional TFET transmission gate based designs. On the other hand, this work leverages the special characteristics of TFET for several hardware security techniques. A new design methodology is introduced that explores TFET p-i-n forward current for hardware obfuscation, true random number generator (TRNG), reconfigurable TRNG and physically unclonable function (PUF), and power analysis countermeasure. Proposed TFET TRNG achieves relatively lower area, low energy consumption of 5.4pJ/bit, and exhibits high robustness against reverse engineering attacks. Further, the ultra-lightweight reconfigurable TRNG and PUF design also achieve low energy consumption of 4.8pJ/bit. A TFET based power analysis countermeasure is presented with low area overhead of 12% and 5% for a single substitution box (S-box) and Advanced Encryption Standard (AES), respectively. Apart from this, TFET steep slope characteristics have been explored to achieve lower energy consumption and enhanced security for differential logic circuits. Proposed TFET differential logic based PRIDE S-box exhibits higher security against power analysis attacks and achieves 3× lower energy consumption compared to FinFET. Moreover, the proposed TFET differential logic-in-memory based logic encryption/locking technique achieves 3× lower energy consumption than FinFET designs.

Keywords: Tunnel FET (TFET), Hardware security, True random number generator (TRNG), Physically unclonable function (PUF), Power analysis attacks, and Hardware obfuscation.

1. Introduction

Hardware security of integrated circuits is become a rising concern due to the emerging new security attacks and breaches [1]. The hardware security attacks, including hardware trojans, reverse engineering, counterfeiting, side-channel analysis and tampering, extract private or secret information from the electronic circuits/systems. Compared to cybersecurity attacks, hardware breaches can be highly damaging because of wide accessibility and resource constraints of internet of things (IoT) devices [2]. In support of this, various global surveys have reported that the cost of counterfeit/malicious goods was estimated in the excess of trillion U.S. dollars and the hardware security modules/systems market is expected to reach approximately 2.03billion U.S. dollars by 2022 due to the rising of serious security attacks on hardware [3]. Besides, the advent of modern security attacks and threats, including hardware trojans, reverse engineering, and side channel attacks, have nullified the underlying notion of the hardware as the root of trust [4]. To avoid the hardware security attacks, several countermeasures have been demonstrated including designing

physically unclonable function (PUF), true random number generator (TRNG), side-channel analysis (SCA) countermeasures, and hardware obfuscation [5-6].

TRNGs that generate statistically independent session keys can be broadly divided into analog and digital TRNGs. Recent digital TRNG designs explore a three-edge multimode ring oscillator (RO), a differential RO with feedback resistors, a tetrahedral ring oscillator, and even stage RO and metastability of digital circuits [7-8]. PUFs have emerged as secure on-the-fly unique key generators that utilize inherent physical variations [9]. PUFs avoid the storing of keys in volatile/non-volatile memory and provide volatile tamper resistant solutions to the key storage. Depending on the size of challenge-response pairs (CRPs), these are classified as weak PUFs and strong PUFs. Strong PUFs include CMOS arbiter PUFs and RO based PUFs, weak PUF are memory based PUFs that exploit metastable states of cross-coupled inverters [9]. Memory-based PUFs were widely designed using CMOS based static random access memory (SRAM) and dynamic random access memory (DRAM). Further, SCA is mainly classified into power analysis, electromagnetic (EM) signal analysis, and photonic emission analysis (PEA). The differential power analysis (DPA) countermeasures explore balanced logic, fully integrated on-chip voltage regulators, CMOS based all-digital low dropout voltage regulator, and CMOS TRNG designs to decorrelate the power and processed data [10]. On the other hand, CMOS based EM attack countermeasures explore modifying crypto engine architecture, power management circuits, and design flow of the IC have been proposed to prevent EM SCA attacks [10]. Similarly, PEA countermeasures like adding an opaque layer, a backside polishing detector and light sensors are also used to identify PEA activities on the chip. Apart from this, hardware obfuscation that hides the original functionality of design has become one of the most popular IC protection techniques. There exist divergent techniques to perform hardware obfuscation including logic encryption/locking, camouflaging, reconfigurable design, and physical design obfuscation [11]. Several hardware security primitive and methodologies have been proposed using existing CMOS technology. However, the existing CMOS technology cannot adequately address the modern security attacks. CMOS based hardware security countermeasures always resulted a high area overhead, performance trade-offs with technology scaling, and required additional design efforts. Hardware security primitives and strategies heavily rely on pre-existing CMOS technologies, which are slowly saturating due to their high leakages in lower channel lengths, emerging new attack models and vulnerabilities.

In support of this, several post-CMOS devices, including tunnel FET (TFET), hybrid phase transition FET (HyperFET), carbon nanotube FET (CNTFET), negative capacitance FET (NCFET), phase-change memory (PCM), spin-transfer torque magnetic tunnel junction (STT-MTJ), resistive random access memory (RRAM) have demonstrated to sustain Moore's law-based performance scaling and/or to improve energy efficiency [12-14]. Among the wide verity of devices, TFETs have proven to be a promising device for building energy-efficient systems at scaled supply voltages [15-16]. TFET works on the principle of

band-to-band tunneling, achieve lower subthreshold swing (<60mV/dec) and high on-current to the off-current ratio (I_{ON}/I_{OFF}) at low supply voltages. As a result, TFET can improve the energy efficiency of digital, analog and RF circuits and become an alternative device candidate to conventional MOSFET [17]. TFET exhibits unique device characteristics such as enhanced miller capacitance effect, negative differential resistance (NDR), p-i-n forward current, and ambipolarity [18]. These special characteristics can be explored with novel designing methodology to avoid the passive role of CMOS technology for hardware security. Several existing CMOS based hardware security countermeasures show significant area overhead and higher energy consumption with increased vulnerability to security attacks [19-22]. To avoid this, several researchers introduced TFET devices into the conventional hardware security countermeasures [23-24]. However, none of the works leverage TFET unique characteristics to develop compact and energy efficient novel circuit architectures for hardware security applications. To address these challenges and technical gaps, this work leverage unique device characteristics of TFET that could drastically simplify circuit architectures and enhance the security against several hardware vulnerabilities.

2. Problem definition and Motivation

With technology scaling, CMOS hardware security countermeasures exhibited large power, area, and delay overhead. Hardware security requires a semiconductor device that exhibits security oriented characteristics with ultra-low energy consumption. The security oriented characteristics need to generate high entropy and unpredictability. In contrast, CMOS device exhibits limited security oriented characteristics and show higher energy consumption at scaled channel lengths. After reviewing several CMOS based hardware security countermeasures, different technical gaps have been identified. Those are explained as follows:

2.1 Technical gaps

The technical gaps of CMOS countermeasures including TRNG, PUF SCA countermeasures, and hardware obfuscation have been discussed below

- CMOS based TRNGs relatively exhibit poor randomness and require large post-processing units, which increases the area and energy consumption. Additionally, the security of CMOS based TRNGs become one of the major concerns.
- CMOS based PUF designs demonstrate three major issues that are the high bit error rate (BER), poor uniqueness and susceptible to temperature variations. Most existing CMOS based PUFs utilize an error-correcting code (ECC) to reduce the final uncertainty. However, strong ECC shows large area overhead and high energy consumption. In spite of being highly secure, CMOS based PUFs are vulnerable to modeling attacks, cryptanalysis attacks, side-channel attacks, and semi-invasive attacks.
- Traditionally, CMOS devices demonstrate high leakage at lower channel lengths due to several second order effects including drain-induced barrier lowering, hot carriers and subthreshold leakage. Consequently, CMOS based systems are highly vulnerable to DPA attacks. The higher static power

consumption of CMOS based balanced logics at sub-50nm can leak confidential information against static power side channel attacks. Moreover, CMOS based SCA countermeasures result in increased power dissipation, area overhead, and complexity.

- Conventional CMOS device properties and design rules of fabricated ICs are easily accessible that makes the attacker's effort easier in delayering the IC. CMOS device characteristics are deterministic and architectures used for systems design are much more conventional. This behavior is highly undesirable for hardware obfuscation applications. Moreover, CMOS based hardware obfuscation techniques exhibit higher power consumption and area overheads.

CMOS based hardware security countermeasures exhibited unavoidable technical gaps and limitations. To address the challenges, novel semiconductor devices that possess an improved energy efficiency with divergent security oriented (special) characterises need to be explored.

2.2 Motivation and Objectives

Alternatively, the emerging TFET devices have achieved lower energy consumption with special characteristics. These special characteristics include ambipolar current, negative differential resistance, p-i-n forward current, superliner on-set, and enhanced miller capacitance. Thus, emerging TFET is considered to design hardware security methodologies that can achieve ultra-low energy consumption with similar security resilience. Thus, the thesis presents the methodology to explore TFET distinct characteristics for hardware security. The main objectives of the thesis are listed below.

i. Designing TFET based digital, analog and RF circuits with ultra-low energy consumption. Exploring TFET device characteristics and investigating their scope for hardware security countermeasures.
ii. Introducing a simplified hardware obfuscation methodology that leverages TFET special characteristics. Demonstration of TFET based compact TRNG that shows lower energy consumption and enhanced security. To avoid the area overhead, a unified design that can work as both TRNG and PUF need to be designed.
iii. Performing the DPA attack on TFET based crypto circuits and retrieving the key information. Exploiting the unique characteristics of TFET, a low area overhead DPA countermeasures required to be designed.
iv. Utilizing TFET steep-slope characteristics for differential logic based hardware secure circuit design to obtain ultra-low energy consumption and enhanced hardware security.

3. Work done in the thesis

This work consists of four different objectives and each contribution starts with the problem statement. Further, different TFET based countermeasures/solutions have been presented for hardware security applications. Moreover, the proposed TFET based designs, results and analysis have been presented in each contribution.

3.1 TFET based ultra-low power and hardware secure circuit design considering p-i-n forward current

TFET exhibits significant p-i-n leakage leading to malfunction in TFET based circuits. However, the effects of p-i-n forward leakage are ignored in the literature, and no deeper insights/techniques have been discussed to reduce its effect. Additionally, CMOS-based security primitives exhibit high power consumption, large area and require additional source/drain doping variations to create stealthy manipulations for hardware obfuscation. Moreover, none of the works explored TFET p-i-n forward current as favourable characteristics in optimizing hardware security countermeasures. This work demonstrates the design of TFET based digital, analog, and RF building blocks. To avoid the increased power consumption and poor reliability due to p-i-n forward current, low-power circuit techniques have been proposed. Further, a new design methodology is presented that leverages TFET p-i-n forward current for hardware obfuscation and optimizing hardware security primitives.

3.1.1 TFET based digital and analog circuit design

Considering the scope of TFET devices, this work demonstrates the TFET based digital and analog building blocks including TFET digital buffer, ring oscillator (RO), and voltage controlled ring oscillator (VCRO). TFET based designs have been benchmarked with industry standard Si FinFET designs. The iso-area, iso-energy, iso-speed and noise margin analyses have demonstrated that TFET buffers are reliable and energy efficient in driving larger loads compared to FinFET buffers. At a supply voltage of 0.2V, the 2-stage TFET buffer achieves 16× higher speed and lower energy consumption compared to FinFET buffers. TFET buffers have exhibited an improved noise margin and proved to be highly capable of nullifying power supply noise effect and signal loss, thereby making the buffer design highly reliable. Additionally, this work presents steep slope TFET based RO and VCRO designs at scaled supply voltages. With the steep slope characteristics of TFET device and smaller delay values, TFET RO exhibits higher frequency of oscillations than FinFET designs. Moreover, TFET based VCRO shows a wide operating frequency range of 13.5 MHz to 135.2 MHz (90%), whereas FinFET based VCRO operates from 15.46 to 22.45MHz (31.13%). The Phase Noise of TFET VCRO is -64.6dB/Hz at 1MHz frequency offset with a low power consumption of 34.12nW and will be suitable for wide frequency range on-chip clock generators/PLLs.

3.1.2 TFET based circuit design considering p-i-n forward current

This work studied the asymmetrical characteristics of TFET and reported that a significant p-i-n forward current is observed with the increase in drain-to-source voltage as shown in Fig. 1(a). TFET shows an identical magnitude of p-i-n forward current by changing gate voltages, as shown in Fig. 1(b). This indicates that as drain-to-source voltage becomes more negative (due to the forward biasing of p-i-n structure), gate loses the control of channel and current is controlled by only drain-to-source voltage. As a result, TFET transmission gate (TG) exhibits unconventional behaviour as shown in Fig. 1(c). Towards this, TFET novel

compact gates and tristate gates have been proposed to mitigate the p-i-n forward current effects. The proposed TFET gates show enhanced reliability in terms of high noise margins and reduced power consumption. The proposed novel compact gate and tristate gate based designs have demonstrated 2× and 6× lower power consumption compared to conventional TFET transmission gate (TG) based designs. Orthogonal to this, a new circuit design methodology is introduced that considered TFET p-i-n forward

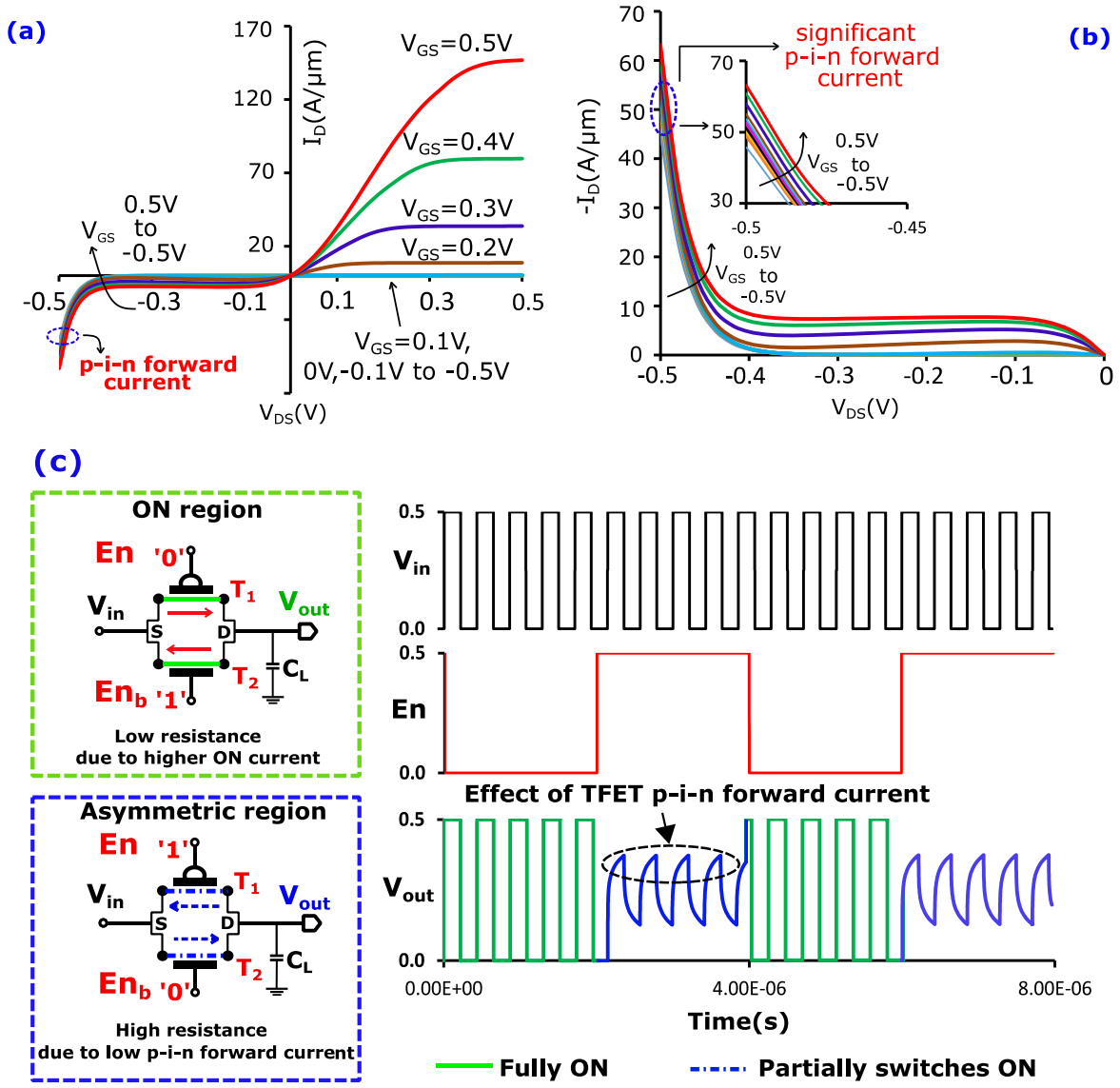

Fig. 1. (a) N-channel TFET drain current characteristics with varying drain-to-source voltage (b) Demonstrating significant p-i-n forward current with negative drain-to-source voltage (c) TFET transmission gate switching mechanism and simulated transient response at 0.5V supply voltage.

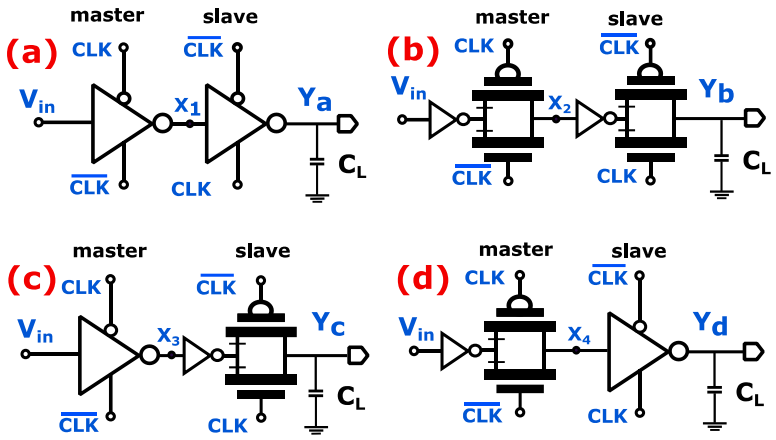

Fig. 2. TFET flip-flop circuits obfuscated to behave as (a) Positive edge-triggered flip-flop (b) Buffer (c) Negative latch (d) Positive latch

Table 1 Summary of proposed TFET flip-flops behavior

Topology	Logic	Functionality
(a)	$Y_a = V_{in}$; When CLK changes from 0 to 1	Flip-flop
(b)	$Y_b = V_{in}$; Independent of CLK	Buffer
(c)	$Y_c = V_{in}$; When CLK=0	Negative Latch
(d)	$Y_d = V_{in}$; When CLK=1	Positive Latch

current as a favourable characteristics for hardware obfuscation applications. TFET p-i-n forward current is utilized to modify the flip-flop functionality for device-level hardware obfuscation application as shown in Fig. 2. Due to the p-i-n forward current of TFET, flip-flops show divergent functionality that is summarized in Table 1. In addition, a new circuit design methodology is demonstrated by exploring TFET p-i-n forward leakage for hardware obfuscation applications. Utilizing the proposed methodology, the optimization of 40% and 80% is achieved in area and power consumption of existing hardware security primitives like TRNGs. However, this contribution ignores the design and analysis of TFET TRNG considering p-i-n forward current. In order to examine the potential of TFET characteristics towards hardware security, the next work demonstrates TFET based TRNG design.

3.2 TFET based TRNG and reconfigurable TRNG/PUF designs

Conventional CMOS based hardware security primitives (TRNG and PUF) exhibit several challenges, specifically in terms of performance, area, energy consumption and design complexity. Moreover, the security of TRNG becomes one of the primary concerns with the advancement of IoT. Circuit topologies/architectures with highly predictable behavior is the key reason behind the development of hardware reverse engineering (RE) that leads to various security attacks like trojan insertion and

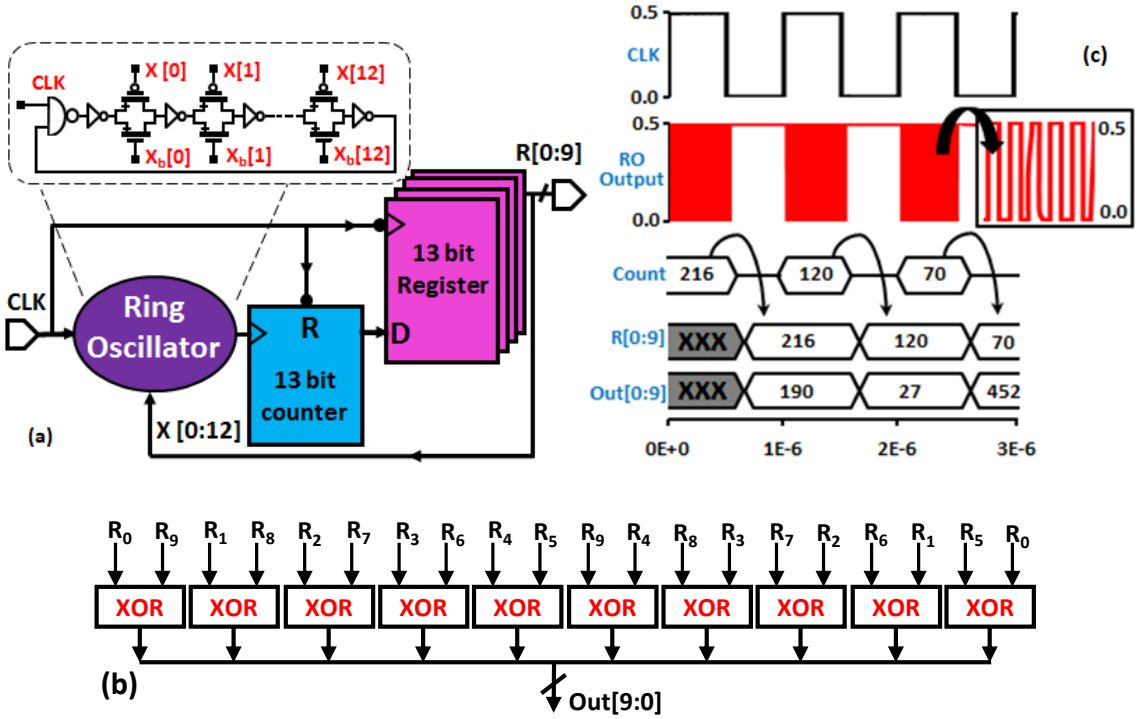

Fig. 3. Proposed (a) TFET p-i-n forward current based TRNG design (b) Post-processing circuit using TFET XOR gates (c) transient characteristics.

counterfeiting. This work presents TFET TRNG, leveraging delay variations of p-i-n forward current based ring oscillator. The proposed TFET TRNG achieves low area and lower energy consumption. Moreover, p-i-n forward current based circuit design makes the proposed TRNG robust against reverse engineering attacks. Furthermore, the ultra-lightweight reconfigurable TRNG and PUF design is also proposed and analyzed.

3.2.1 TFET based TRNG design

The p-i-n forward current in emerging TFET devices directly depends on the doping concentration and several other device parameters. Thus, the p-i-n forward current based circuit design makes reverse engineering very slow and expensive process. Considering this, emerging TFET based energy efficient true random generator is designed that exhibits high resilience towards reverse engineering attacks. TFET TG functionality failure due to the p-i-n forward current is exploited for TRNG circuit design. Exploiting the TFET TG functional failure, TFET p-i-n forward current based RO design is proposed. It is demonstrated that the frequency of oscillations of proposed RO varies depending on the number of TFET TGs in the asymmetrical region and pattern in which the control bits are applied. Leveraging TFET RO as a source of randomness, TFET TRNG is designed as shown in Fig. 3(a). Figure 3(b) depicts the XOR gate based post-processing unit, used to increase the randomness of TRNG output. From the transient characteristics, it can

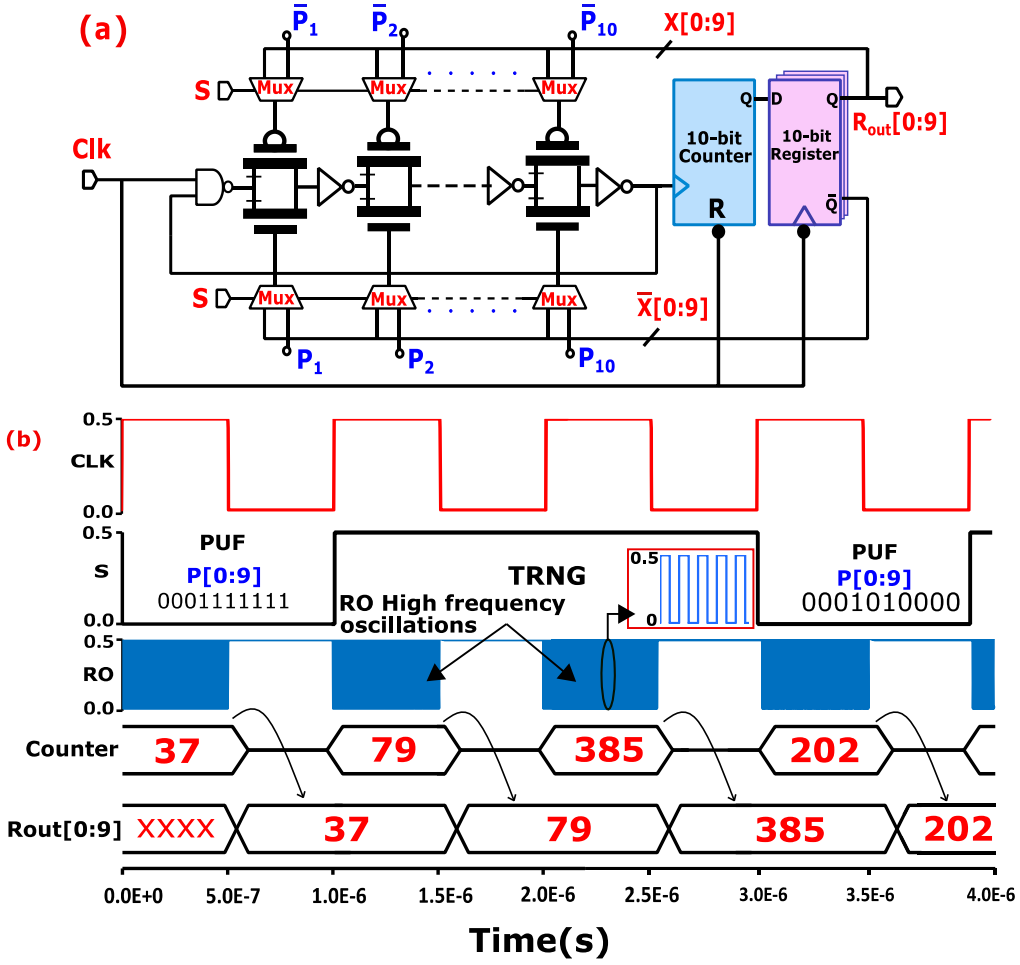

Fig. 4. Proposed TFET based reconfigurable PUF and TRNG (a) Circuit design (b) Transient characteristics.

be observed that TRNG exhibited random sequence as shown in Fig. 3(c). The obtained output sequence of TRNG and it's entropy is observed to be random. A complete national institute of standard and technology (NIST) test is performed on harvested 100kb random bits of TRNG and the design passed various tests. The performance of TFET TRNG is compared with existing designs as shown in Table 2.

3.2.2 TFET based reconfigurable TRNG and PUF design

Further, TFET based reconfigurable TRNG and PUF design is demonstrated (as shown in Fig. 4(a)) that leverages the special p-i-n forward characteristics of the device. Selection line '*S*' is responsible for operating the proposed design either as PUF or TRNG with the help of multiplexers. The functionality of the reconfigurable PUF and TRNG design can be well understood from the transient response as shown in Fig. 4(b). This unique behavior encouragingly leads to the unpredictable frequency of oscillations in TFET RO that act as a main source of entropy for both PUF and TRNG. The PUF is designed by exploring a unique methodology that considers variation in TFET p-i-n forward current. At lower supply voltages of

Table 2 Performance comparison of proposed design with existing literature

Parameter	[8]	[8]	[7]	[19]	This work	This Work
Method	Oscillator collapse	Oscillator collapse	Oscillator jitter	FinFET Metastability	TFET p-i-n forward current	TFET p-i-n forward current
Design	PUF	TRNG	TRNG	Unified TRNG/PUF	TRNG design	Reconfigurable TRNG/PUF
Technology (nm)	40	40	28	14	20	20
V_{DD} (V)	0.5	0.9	0.9	0.65	0.5	0.5
Power consumption (µW)	28.4	46	540	72.54	54	48
Energy consumption (pJ/bit)	17.75	23	23	7.25	5.4	4.8
Gate equivalent (#)	2517	2458	502	1181	388	417
Bitrate (Mb/s)	1.6	2	23.16	1480	10	10
Variation effect (Temperature, Voltage)	Considered	Considered	Considered	Considered	Not considered	Considered

[#]Gate equivalent is calculated by standardizing all TRNG designs to 10-bit and considered the static inverter as reference gate

0.5V and 0.45V, the proposed PUF has shown a higher degree of uniqueness 47.5% and 46%, respectively. Further, PUF exhibited a high reliability of 82% and 88.7% with supply voltage and temperature variations, respectively.

The proposed TRNG and reconfigurable TRNG/PUF designs exhibited lower gate count and low energy consumption when compared with existing countermeasures, as shown in Table 2. Proposed TFET TRNG exhibits lower gate count and low energy consumption of 5.4pJ/bit at 0.5V compared to other designs. Additionally, the behavior of TRNG mainly depends on the magnitude of p-i-n forward current that makes TFET TRNG design robust against reverse engineering attacks. The reconfigurable TRNG and PUF design demonstrated lower gate count with an energy consumption of 4.8pJ/bit at 0.5V. Thus, the proposed designs achieve lower area overhead and lower energy consumption. However, this work ignores the other important hardware security breach that is power analysis attack on cryptographic circuits. Henceforth, the next contribution demonstrates the differential power analysis attack on TFET based cryptographic circuit and proposed a feasible countermeasure.

3.3 A low area overhead TFET based DPA countermeasure

Traditionally, CMOS devices exhibit high leakage at lower channel lengths due to several second order effects including drain-induced barrier lowering, hot carriers and subthreshold leakage. Consequently, CMOS based systems are highly vulnerable to differential power analysis (DPA) attacks. Moreover, CMOS based countermeasures often exhibit high delay, area overhead and require extensive design efforts. To avoid this, a low area overhead DPA countermeasure is demonstrated exploring TFET based random

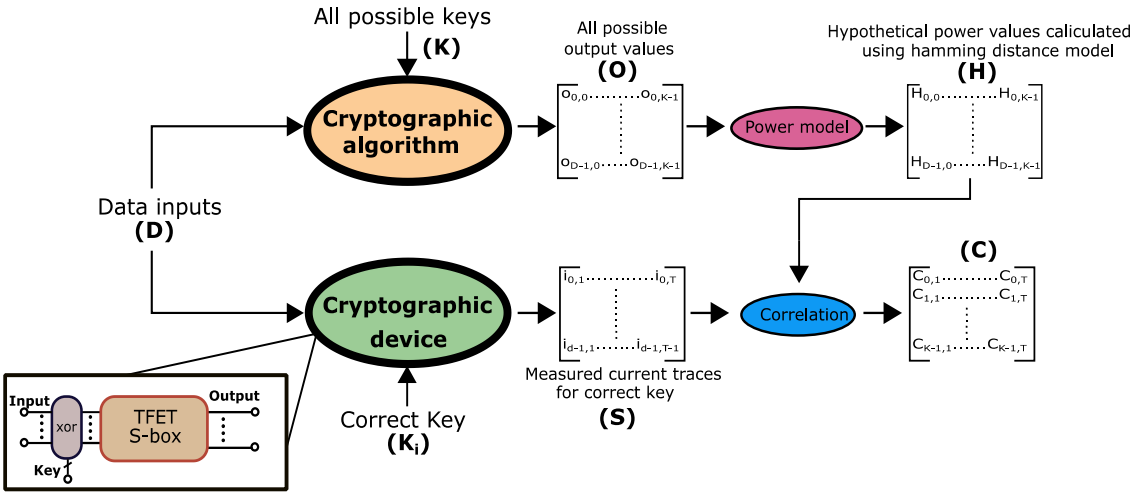

Fig. 5. DPA attack mechanism on TFET based S-box.

number generator. The proposed DPA countermeasure is designed by integrating the original TFET substitution box (S-box) and TFET RNG.

3.3.1 TFET based DPA countermeasure

Personal information stored in IoT devices is highly vulnerable to side-channel attacks (SCA) due to their wide distribution and easier physical access. Among the various side-channel analysis attacks demonstrated, DPA is powerful due to its simple setup and effectiveness in recovering the secret key information. The attack mechanism of DPA on S-box design is depicted in Fig. 5. DPA discloses the secret key stored in cryptographic engines by using multiple power traces. Orthogonal to current CMOS based countermeasures, this work investigates TFET device characteristics to reduce area overheads while

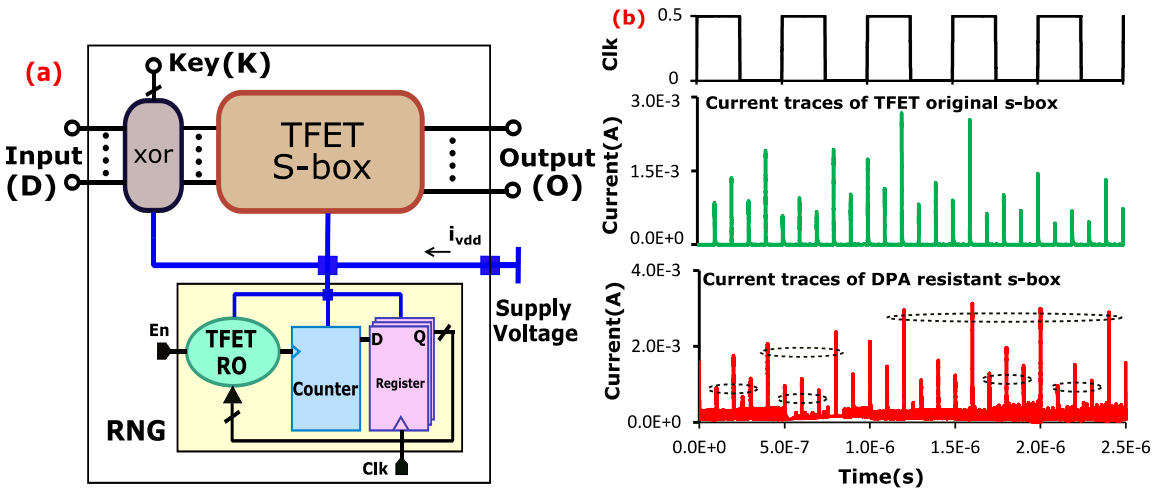

Fig. 6. (a) Architecture of TFET based DPA Resistant S-box (b) Power traces.

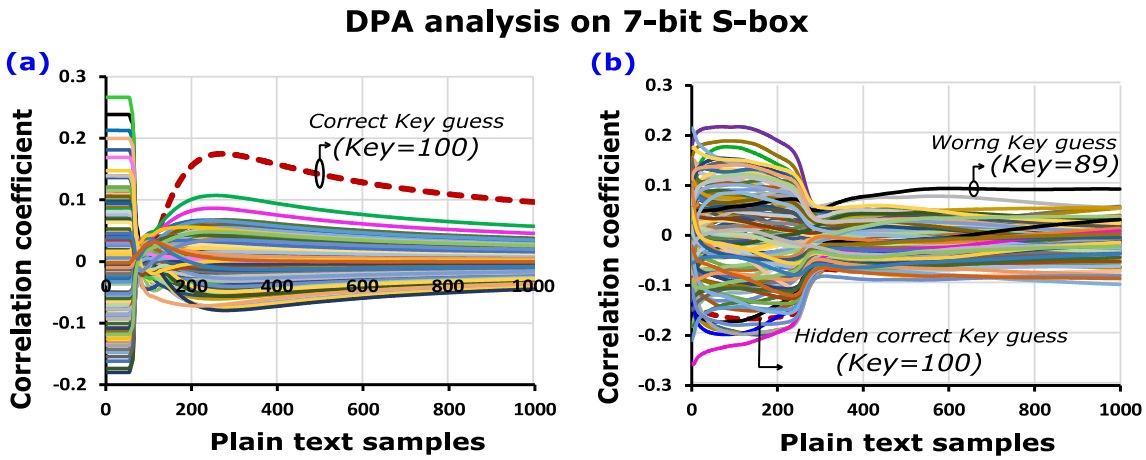

Fig. 7. Correlation coefficients of (a) Original TFET 7-bit S-box (b) TFET based DPA resistant 7-bit S-box.

achieving a similar level of DPA resilience. A low area overhead DPA countermeasure is demonstrated exploring emerging TFET based random number generator (RNG). TFET TG exhibits unconventional behavior due to p-i-n forward current of the device. These TFET TG designs, connected as a cascaded chain exhibited non-linear propagation delay values. This propagation delay of TFET TG is mathematically modelled and verified with simulation results. Leveraging this behavior, a compact TFET RNG is designed that extracts random bits from delay variations of the TFET ring oscillator. The proposed TFET RNG achieves low area overhead when compared with the baseline CMOS designs. Further, a 7-bit substitution box (S-box) that is used in Advanced Encryption Standard (AES) algorithm has been implemented using 20nm InAs TFET. The power traces of TFET S-box design are extracted and sampled. A python-based simulation framework is developed to perform the DPA attack and the secret key of unprotected TFET S-box was successfully disclosed. The TFET DPA resistant S-box architecture is designed by integrating the original TFET S-box and proposed RNG as shown in Fig. 6(a). Multiple current traces of TFET original S-box and TFET DPA resistant S-box are collected as shown in Fig. 6(b). From Fig. 7(a), it can be observed that the DPA attack performed on TFET original 7-bit S-box is successful, indicating that the correlation coefficient of the correct key (K=100) is higher than the remaining keys. On the other hand, an attack performed on TFET DPA resistant 7-bit S-box (Fig. 7(b)) is observed to be unsuccessful, indicating that the correlation coefficient of the wrong key (K=89) is higher. Furthermore, the correct key K=100 does not result in a high correlation and is hidden in the analysis result. The proposed TFET based DPA countermeasures is compared with the existing designs as shown in Table 3. The Overall area overhead of the proposed S-box design is 12%, which is low compared to the existing countermeasures. This low area overhead is obtained by exploiting the special characteristics of TFET. Moreover, the proposed design results no additional delay (0%) as the TFET RNG works in parallel with S-box design. At a supply voltage of 0.5V, the proposed design shows 3.77× increment in power consumption. Furthermore, the overall area

Table 3 Performance comparison of proposed DPA countermeasure

Parameter		[20]	[21]	[22]	This work
Method		CMOS SABL logic	FinFET Adiabatic logic	CMOS Ring oscillator	TFET RNG
Technology(nm)		90	20	90	20
Supply voltage(V)		1	0.9	1.2	0.5
Gate equivalent [#]	Original design	822	1101	637	1150
	DPA resistant design	1748	1812	758	1297
Area overhead (%)		112	64.5	19	12
Power consumption (μW)	Original	-	-	150	18
	DPA resistant	-	-	600	68
Power increment (in times)		-	-	4	3.77
Delay overhead (%)		-	-	0	0

Basic static inverter design is assumed when comparing gate equivalent

overhead of AES core is estimated as 5% by using the proposed method. Thus, TFET based DPA countermeasures shows lower area overhead. However, this work ignores differential logic based DPA countermeasures. Moreover, prior works have not designed the circuits of TFET with other technologies (heterogeneous technologies based circuit designed). Therefore, the STT-MTJ based logic-in-memory (LiM) cells have been proposed by using TFET and explored them for logic locking/encryption applications in next work.

3.4 TFET differential logic based hardware secure circuit design

Existing CMOS sense amplifier logic (SABL) is proved to be secure and shows several challenges, including higher power and energy consumption. Moreover, at sub-50nm channel lengths, CMOS SABL exhibited higher static power consumption and become highly vulnerable to static power side channel attacks. Besides, STT-MTJ based LiM circuits exhibited large energy consumption due to the poor performance of MOS devices at scaled channel lengths (or supply voltages). Consequently, recent STT-MTJ LiM cells based crypto circuits exhibited increased energy consumption overhead. To reduce the energy consumption, emerging TFET is introduced into the differential logic circuits that achieved ultra-low energy consumption while maintaining higher security. TFET SABL gates based cryptographic circuits have been proposed to achieve lower energy consumption than FinFET designs with higher DPA resilience. Besides, spin transfer torque magnetic tunnel junction (STT-MTJ) and TFET based logic-in-memory (LiM) gates have been demonstrated for logic encryption/locking and compared with STT-MTJ and FinFET designs.

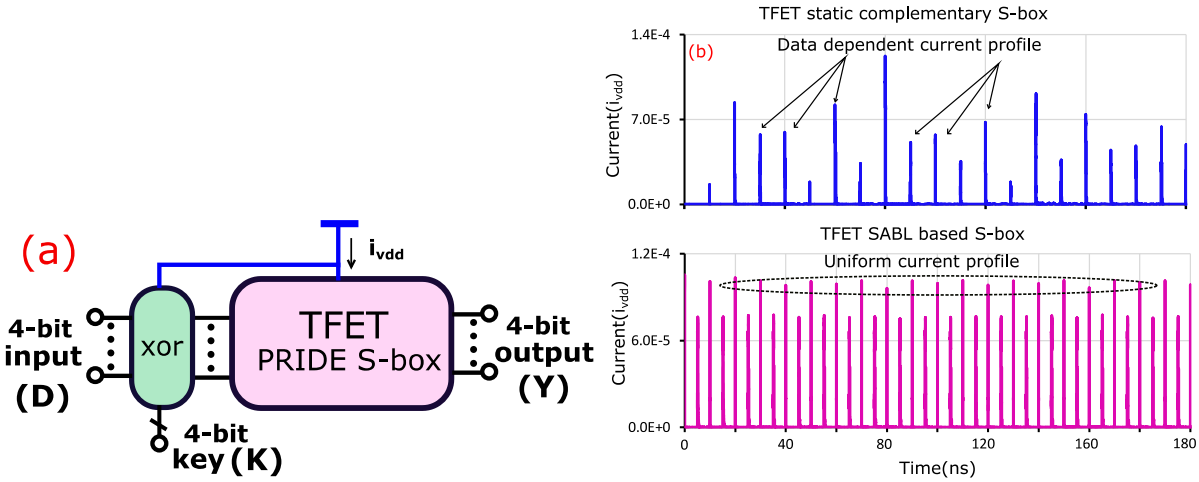

Fig. 8. (a) Proposed TFET based PRIDE S-box design (b) Power traces.

3.4.1 TFET SABL based DPA resilient circuits design

Existing CMOS technology with scaled channel lengths exhibited several challenges in designing hardware secure electronic circuits with ultra-low energy consumption. CMOS differential power analysis (DPA) countermeasures exploring sense amplifier based logic (SABL) presents higher energy consumption and increased vulnerability to security attacks. Additionally, STT-MTJ and CMOS based LiM cells demonstrate high energy consumption overhead due to the large write current of STT-MTJ and poor MOS device performance at scaled channel lengths. In this work, TFET steep-slope device characteristics have been leveraged for hardware security techniques that achieve ultra-low energy consumption at lower supply voltages. To avoid the CMOS challenges, TFET based SABL gates have been proposed that achieve 3× lower energy consumption compared to Si FinFET SABL designs. Further, utilizing TFET SABL gates, TFET PRIDE S-box is designed and power traces have collected as shown in Fig. 8. With the collected power traces, the DPA attack is performed on TFET SABL and TFET static complementary S-box designs. Figure 9 shows the correlation coefficients characteristics, indicating higher DPA resilience of TFET SABL

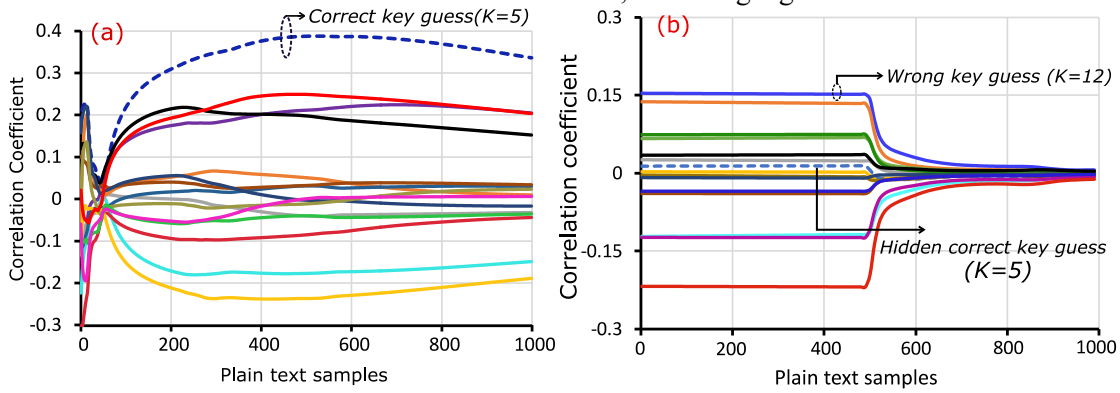

Fig. 9. Correlation coefficient of (a) TFET based static complementary S-box design (b) TFET SABL based S-box design

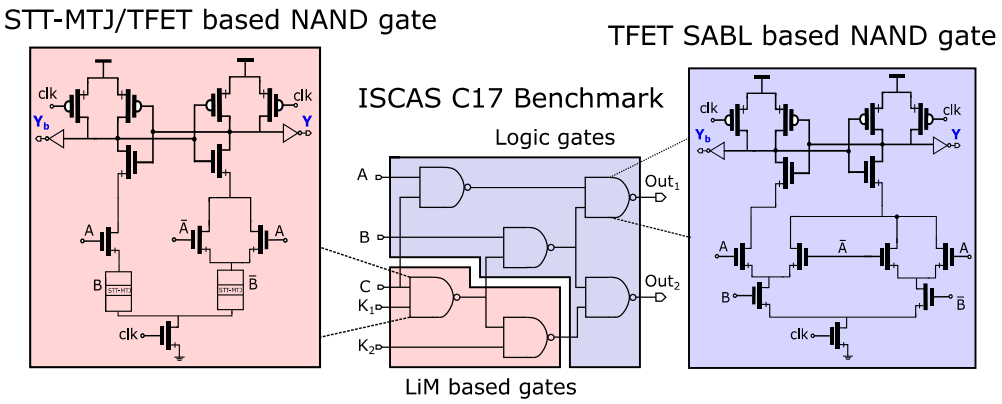

Fig. 10. STT-MTJ and TFET based ISCAS C17 benchmark explored for logic locking application.

based S-box. Moreover, TFET SABL based S-box achieves 3.15× lower energy consumption compared to FinFET designs with higher DPA resilience. With lower static power consumption, TFET SABL based crypto systems show lower vulnerability to static power side-channel attacks.

3.4.2 STT-MTJ and TFET LiM gates based logic locking/encryption

STT-MTJ based LiM circuits exhibited large energy consumption due to the poor performance of MOS devices at scaled channel lengths (or supply voltages). To avoid this, STT-MTJ and TFET LiM gates have been proposed that achieve 4× lower energy consumption compared to STT-MTJ and FinFET designs. Moreover, these STT-MTJ and TFET LiM gates have been explored in the logic encryption/locking technique. For example, consider ISCAS C17 benchmark (Fig. 10) that is explored for logic locking application. The TFET and STT-MTJ logic encryption/locking benchmark circuit shows 3.11× lower energy consumption compared to STT-MTJ and FinFET design. Moreover, the TFET technology can show the ease of integration and flexibility in manufacturing with STT-MTJ. However, secondary effects including ambipolarity, p-i-n forward current and enhanced miller effect still exist in TFET which make it unpopular and less suitable for commercialization now. More research efforts are required to make these emerging technology integration a reality.

4. Conclusion and Future scope

The complete work can be summarized as follows. This work initially presents the design and benchmarking of TFET based basic digital, analog, and RF building blocks. Further, low-power circuit techniques have been demonstrated to mitigate the p-i-n forward current effects. Apart from this, p-i-n forward current is explored for optimizing hardware security primitives and hardware obfuscation applications. Later, a TFET TRNG is designed that achieves lower area and lower energy consumption. Moreover, p-i-n forward current based circuit design makes the proposed TRNG robust against reverse engineering attacks. Further, the ultra-lightweight reconfigurable TRNG and PUF design is also proposed and analyzed. Additionally, a low area overhead DPA countermeasure is designed exploring TFET based

Table 4 Summary of proposed TFET based hardware security countermeasures and benchmarking

Design		Parameters	TFET	CMOS/FinFET (Equivalent designs are considered)	Other security benefits using TFET special characteristics	Contributing chapter in the thesis
TFET basic building blocks	Buffer	Energy consumption(aJ)	8.47	137	-	Chapter 3
	RO	Maximum Frequency of oscillations(GHz)	21	13		
	VCRO	Tuning range(MHz)	13.5-135.2 (90%)	15.46-22.45 (31%)		
Hardware security primitives		Power consumption(µW)	4	15	Variations due to inherent characteristics	Chapter 3
		Gate equivalent	92	152		
Flip-Flop design for obfuscation		Device-level hardware obfuscation	Inherent characteristics	Separate drain/source doping changes required	High resilience towards the scanning electron microscope	Chapter 3
TRNG Design		FoM (pJ/bit) (Power consumption/bit rate)	5.1	23	Robust against reverse engineering attacks	Chapter 4
		Gate equivalent	315	502		
DPA Countermeasure		Area Overhead for S-box design	12%	19%	Higher resistance to power analysis attacks	Chapter 5
SABL based PRIDE S-box		Energy consumption(fJ)	13.09	41.339	Higher resistance to power analysis attacks	Chapter 6
TFET STT-MTJ based Logic encryption circuit			6.96	21.64	-	

random number generator. The proposed architecture is found to be resilient to DPA attack and the area overhead of a single S-box and AES is observed to be lower without any extra delay. To reduce the energy consumption of CMOS SABL based circuits and CMOS based STT-MTJ LiM cells, emerging TFET is introduced into these circuits that achieved ultra-low energy consumption while maintaining similar security level. Table 4 summarizes the important results that are obtained from the main contributions of this work. From this, it can be observed that TFET based hardware security primitives/techniques show a clear improvement in energy consumption and area overhead compared to FinFET/CMOS designs.

Moreover, TFET designs achieve additional security benefits. These advantages are due to the special characteristics of the TFET that are utilized for circuit designs. Inherent TFET p-i-n forward current makes circuits/systems robust against several attacks, including reverse engineering, power analysis and cloning attacks.

Apart from the above benefits, this work can be improved and extended in different directions. For beyond-CMOS based research, the compact model development of nanoelectronic devices has become a cornerstone in estimating the circuit/system performance. Consequently, this work can be extended to design a compact model with high speed execution and higher accuracy. In order to reap the full benefits of beyond-CMOS device technologies, this work can extend towards the selective integration of emerging technologies that exhibit lower energy consumption with enhanced hardware security. Apart from the simulation results, the experimental verification is very important to observe the real-time challenges and benefits of TFET based circuits. In this view, this work can be extended to validate the results through fabrication and gate level design using field programmable gate arrays (FPGAs). Different performance parameters like power consumption and LUTs required can be estimated for the designed architectures.

5. Thesis organization

The thesis consists of seven chapters starting from the introduction and ending with the conclusion. Each chapter starts with a brief introduction and ends with a summary. Moreover, results and comparisons with the existing countermeasures (literature) have been presented at the end of each chapter. A brief discussion about each chapter is listed below.

Chapter 1 presents the brief introduction of the thesis. The significance of hardware security and challenges of CMOS technology in implementing hardware security primitives/methodologies have been discussed. Further, different beyond-CMOS devices that are proposed in the literature have been presented. Moreover, the problem definition, motivation, and outline of the work have been demonstrated at the end.

Chapter 2 explains about recent trends and advances of CMOS hardware security primitives and methodologies, particularly true random number generators, physically unclonable functions, side-channel analysis countermeasures, and hardware obfuscation techniques. First, the basic functionality and operation of hardware security primitives/methodologies are explained. Later, CMOS technology challenges for the design of hardware security primitives and methodologies have been reported. Finally, the challenges and drawbacks of CMOS countermeasures have been identified.

Chapter 3 demonstrates the design of TFET based digital, analog, and RF building blocks. The analysis of TFET design is performed and compared with industry standard FinFET. Moreover, low-power circuit techniques have been proposed that result in novel compact gates and recommends tristate gates to mitigate the impact of p-i-n forward current. Further, a new design methodology is introduced that leverages TFET

p-i-n forward current for hardware obfuscation applications. Utilizing the proposed design methodology, the optimization in area and power consumption of hardware security primitives is also accomplished.

Chapter 4 presents TFET TRNG harvesting random bits from delay variations of p-i-n forward current based ring oscillator. The proposed TRNG has been tested using NIST test suit and compared with the existing literature. The proposed TFET TRNG exhibits low area and achieves lower energy consumption. Moreover, p-i-n forward current based circuit design makes the proposed TRNG robust against reverse engineering attacks. Further, the ultra-light weight reconfigurable TRNG and PUF design is also proposed and analyzed.

Chapter 5 demonstrates a low area overhead DPA countermeasure exploring TFET based random number generator. The proposed DPA countermeasure is demonstrated by integrating the original TFET substitution box (S-box) and TFET RNG. The proposed architecture is found to be resilient to DPA attack and the area overhead of a single S-box and AES is relatively low.

Chapter 6 leverages TFET steep-slope device characteristics for differential logic based hardware security techniques. To reduce the energy consumption, emerging TFET is introduced into sense amplifier based logic (SABL) circuits that achieved ultra-low energy consumption with enhanced security. TFET SABL based gates and PRIDE S-box design achieve approximately 3× lower energy consumption compared to FinFET designs while maintaining higher DPA resilience. The proposed STT-MTJ and TFET LiM gates have been explored in logic encryption/locking technique that shows 3× lower energy consumption compared to STT-MTJ and FinFET designs.

Chapter 7 offers conclusions. The conclusions are provided based on the work and analysis performed in each chapter. Further, the future scope of the thesis is also discussed.

6. List of publications

International Journals:

1. **J. Aditya**, M. K. Majumder, S. K. Sahoo, and R. Vaddi, "An Ultra-lightweight reconfigurable TRNG and PUF Design exploring TFET p-i-n forward current Characteristics" *International Journal of Circuit Theory and Applications, Wiley*, 2021 (SCI Indexed, IF = 1.58) [In press].

2. **J. Aditya**, M. K. Majumder, S. K. Sahoo, R. Vaddi, and B. K. Kaushik, "Hardware Security exploiting post-CMOS Devices: Fundamental device characteristics, State-of-the-Art Countermeasures, Challenges and Roadmap" *IEEE Circuits and Systems Magazine*, 2020 (SCI Indexed, IF = 2.679) [Accepted].

3. **J. Aditya**, M. K. Majumder, S. K. Sahoo and R. Vaddi, "Low area overhead DPA countermeasure exploiting tunnel transistor-based random number generator" *IET Circuits, Devices Systems*, vol. 14, no. 5, pp. 640-647, 2020 (SCI Indexed, IF = 1.29) [Published]. DOI: 10.1049/iet-cds.2019.0504.

4. **J. Aditya**, M. K. Majumder, S. K. Sahoo, and R. Vaddi, "Tunnel FET-based ultra-low power and hardware-secure circuit design considering p-i-n forward leakage", *International Journal of Circuit Theory and Applications, Wiley*, vol. 48, no. 4, pp.524-538, 2020 (SCI Indexed, IF = 1.58) [Published]. DOI: 10.1002/cta.2731.

5. **J. Aditya**, M. K. Majumder, S. K. Sahoo and R. Vaddi, "Tunnel FET ambipolarity based energy efficient and robust true random number generator against reverse engineering attacks" *IET Circuits, Devices Systems,* vol. 13, no. 5, pp. 689-695, 2019 (SCI Indexed, IF = 1.29) [Published]. DOI: 10.1049/iet-cds.2018.5297.

6. **J. Aditya**, M. K. Majumder, S. K. Sahoo, and R. Vaddi, "Emerging Tunnel FET and Spintronics based Hardware Secure Circuit Design with Ultra-low Energy Consumption" *Journal of computational electronics, Springer*, 2020 [Revision resubmitted].

International Conferences:

1. **J. Aditya**, M. K. Majumder, S. K. Sahoo, P. Yellappa, J. R. Choi and R. Vaddi, "A Low Voltage Discriminant Circuit for Pattern Recognition Exploiting the Asymmetrical Characteristics of Tunnel FET" *In Proc.: IEEE International Symposium on Circuits and Systems (ISCAS)*, Sevilla, 2020, pp. 1-5. [Published]. DOI: 10.1109/ISCAS45731.2020.9180724.

2. **J. Aditya**, T. Nagateja, S. K. Vishvakarma, P. Yellappa, J. R. Choi and R. Vaddi, "Tunneling Field Effect Transistors for Enhancing Energy Efficiency and Hardware Security of IoT Platforms: Challenges and Opportunities" *In Proc.: IEEE International Symposium on Circuits and Systems (ISCAS)*, Florence, 2018, pp. 1-5. [Published]. DOI: 10.1109/ISCAS.2018.8350939.

3. **J. Aditya**, T. Nagateja, and R. Vaddi, "Tunneling Field Effect Transistors for Energy Efficient Logic, Sensor Interface and 3D IC Circuits for IoT Platforms" *In Proc.: IEEE International Symposium on Nanoelectronic and Information Systems (iNIS)*, Bhopal, 2017, pp. 90-92. [Published]. DOI: 10.1109/iNIS.2017.28.

4. **J. Aditya**, V. Harshita, and R. Vaddi, "Exploiting Characteristics of Steep Slope Tunnel Transistors Towards Energy Efficient and Reliable Buffer Designs for IoT SoCs," *In Proc.: Springer International Symposium on VLSI Design and Test,* Singapore, 2017, pp. 259- 269. [Published]. DOI: doi.org/10.1007/978-981-10-7470-726.

5. **J. Aditya**, S. Sadulla , and R. Vaddi, "Exploiting the steep subthreshold slope characteristics of tunnel transistors for wide tuning range VCRO design at scaled supply voltages down to 150mV" *In Proc.: IEEE International Conference on Emerging Electronics (ICEE)*, Mumbai, 2016, pp. 1- 2. [Published]. DOI: 10.1109/ICEmElec.2016.8074564.

Book Chapter and Book:

1. **J. Aditya**, T. Nagateja and R. Vaddi, "Tunneling field effect transistors for energy efficient digital, RF and power management circuit designs enabling IoT edge computing platforms" *VLSI and Post-CMOS Electronics: Design, modelling and simulation, IET*, vol 1, 2019, pp. 263-283. DOI: 10.1049/PBCS073Fch.

2. M. K. Majumder, V. R. Kumbhare, **J. Aditya**, and B. K. Kaushik, Introduction to Microelectronics to Nanoelectronics: Design and Technology, *CRC Press, Taylor & Francis*, 2020.

7. References

[1] A. Sengupta, and S. P. Mohanty, "IP core protection and hardware-assisted security for consumer electronics", *Institution of Engineering and Technology*, March 2019.

[2] T. Hoque, R. S. Chakraborty and S. Bhunia, "Hardware Obfuscation and Logic Locking: A Tutorial Introduction," *IEEE Design & Test*, vol. 37, no. 3, pp. 59-77, June 2020.

[3] M. Bartock, M. Souppaya, R. Savino, T. Knoll, U. Shetty, M. Cherfaoui, R. Yeluri, and K. Scarfone, "Hardware-Enabled Security for Server Platforms: Enabling a Layered Approach to Platform Security for Cloud and Edge Computing Use Cases," *National Institute of Standards and Technology*, pp. 39-39, 2020.

[4] The Cost of Malicious Cyber Activity to the US Economy, W. House, 2018. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

[5] S. Khan, A.P.Shah, S.S. Chouhan, J.G. Pandey, and S. K. Vishvakarma, "D flip-flop based TRNG with zero hardware cost for IoT security applications", *Microelectronics Reliability*, vol. 120, pp.114098, May 2021.

[6] F. Rahman, B. Shakya, X. Xu, D. Forte and M. Tehranipoor, "Security Beyond CMOS: Fundamentals, Applications, and Roadmap," *IEEE Transactions on VLSI Systems*, vol. 25, no. 12, pp.3420-3433, Dec. 2017.

[7] K. Yang, D. Fick, M. B. Henry, Y. Lee, D. Blaauw and D. Sylvester, "A 23Mb/s 23pJ/b Fully Synthesized True-Random-Number Generator in 28nm and 65nm CMOS," in *Proc. IEEE International Solid-State Circuits Conference Digest of Technical Papers*, San Francisco, CA, pp. 280-281, Feb. 2014.

[8] K. Yang, D. Blaauw and D. Sylvester, "An All-Digital Edge Racing True Random Number Generator Robust Against PVT Variations," *IEEE Journal of Solid-State Circuits*, vol. 51, no. 4, pp. 1022-1031, April 2016.

[9] V. P. Yanambaka, S. P. Mohanty and E. Kougianos, "Making Use of Manufacturing Process Variations: A Dopingless Transistor Based-PUF for Hardware-Assisted Security," *IEEE Transactions on Semiconductor Manufacturing*, vol. 31, no. 2, pp. 285-294, May 2018.

[10] A. Singh, M. Kar, S. Mathew, A. Rajan, V. De and S. Mukhopadhyay, "A 128bit AES Engine with Higher Resistance to Power and Electromagnetic Side-Channel Attacks Enabled by a Security-Aware Integrated All-Digital Low-Dropout Regulator," in *Proc. IEEE International Solid-State Circuits Conference Digest of Technical Papers*, San Francisco, CA, pp.404-406, Feb. 2019.

[11] A. Vijayakumar, V. C. Patil, D. E. Holcomb, C. Paar and S. Kundu, "Physical Design Obfuscation of Hardware: A Comprehensive Investigation of Device and Logic-Level Techniques," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 1, pp.64-77, Aug. 2016.

[12] S. Kanungo, B. Majumdar, S. Mukhopadhyay, D. Som, S. Chattopadhyay and H. Rahaman, "Investigation on the Effects of Substrate, Back-Gate Bias and Front-Gate Engineering on the Performance of DMTFET-Based Biosensors," *IEEE Sensors Journal*, vol. 20, no. 18, pp. 10405-10414, Sept. 2020.

[13] B. Sharma, C. Kundu, H. Rahaman, and C. K. Sarkar, "Study of TMR with Different Ferromagnetic Material and Variations in Spin-Split, Thickness and Oxide Barrier Height of a MTJ Memory Device" *Journal of Nanoelectronics and Optoelectronics*, vol. 13*,* no. 2, pp.245-250, Feb. 2018.

[14] N. Bagga, N. Chauhan, A. Bulusu and S. Dasgupta, "Demonstration of a Novel Ferroelectric-Dielectric Negative Capacitance Tunnel FET," in *Proc. IEEE Conference on Modeling of Systems Circuits and Devices (MOS-AK India)*, Hyderabad, India, pp. 102-105, Feb. 2019.

[15] M. Yadav, A. Bulusu, and S. Dasgupta, "Two dimensional analytical modeling for asymmetric 3T and 4T double gate tunnel FET in sub-threshold region: Potential and electric field," *Microelectronics Journal*, vol. 44, no.12, pp.1251-1259, Dec. 2013.

[16] S. Kanungo, S. Chattopadhyay, P. S. Gupta, K. Sinha and H. Rahaman, "Study and Analysis of the Effects of SiGe Source and Pocket-Doped Channel on Sensing Performance of Dielectrically Modulated Tunnel FET-Based Biosensors," *IEEE Transactions on Electron Devices*, vol. 63, no. 6, pp. 2589-2596, June 2016.

[17] A. Beohar, N. Yadav, A. P. Shah, and S. K. Vishvakarma, "Analog/RF characteristics of a 3D-Cyl underlap GAA-TFET based on a Ge source using fringing-field engineering for low-power applications," *Journal of Computational Electronics*, vol. 17, no. 4, pp.1650-1657, Dec. 2018.

[18] S. Saurabh, and J. M. Kumar, "Fundamentals of Tunnel field-effect Transistors," *CRC press*, 2016.

[19] S. K. Satpathy et al., "An All-Digital Unified Physically Unclonable Function and True Random Number Generator Featuring Self-Calibrating Hierarchical Von Neumann Extraction in 14-nm Tri-gate CMOS," *IEEE Journal of Solid-State Circuits*, vol. 54*,* no. 4, pp. 1074-1085, April 2019.

[20] E. Tena-Sanchez, J. Castro and A. J. Acosta, "A Methodology for Optimized Design of Secure Differential Logic Gates for DPA Resistant Circuits," *IEEE Journal on Emerging and Selected Topics in Circuits and Systems*, vol. 4, no. 2, pp. 203-215, June 2014.

[21] S. D. Kumar, H. Thapliyal, and A. Mohammad, "FinSAL: A novel FinFET based Secure Adiabatic Logic for energy-efficient and DPA resistant IoT devices," *IEEE Transactions on Computer-Aided Design Integrated Circuits and Systems*, vol. 37, no. 1, pp. 110–122, March 2017.

[22] P. Liu, H. Chang and C. Lee, "A Low Overhead DPA Countermeasure Circuit Based on Ring Oscillators," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 57, no. 7, pp. 546-550, July 2010.

[23] A. Chen, X. S. Hu, Y. Jin, M. Niemier, and X. Yin, "Using Emerging Technologies for Hardware Security Beyond PUFs," in *Proc. IEEE Conference on Design, Automation & Test,* Dresden*,* pp. 1544-1549, March 2016.

[24] Y. Bi, K. Shamsi, J. S. Yuan, Y. Jin, M. Niemier and X. S. Hu, "Tunnel FET Current Mode Logic for DPA-Resilient Circuit Designs," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 3, pp. 340-352, April 2016.